3 操作の基本

セキュリティ

本装置には、新しいリモート管理機能が備えられています。この機能を使用するには、本装置のネットワーク・インターフェースにIPアドレスを割り振る必要があります。したがって、セキュリティも、配慮すべき問題の1つとして考えなければなりません。リモートで本装置を管理する場合は、第6章「リモート管理」の「アクセス制御」の節を必ずお読みください。

単一サーバ・アクセラレーション

本装置は、単一のサーバへのSSL処理の要求に対処する構成で使われる場合があります。単一サーバ構成は、最も単純なサーバ構成です。このサーバ構成では、本装置をルータとサーバの間にあるネットワークに接続します。設置においては、セキュリティを高め、管理をしやすくするために、本装置とサーバを同じラックに配置する等、近距離に配置することを心がける必要があります。

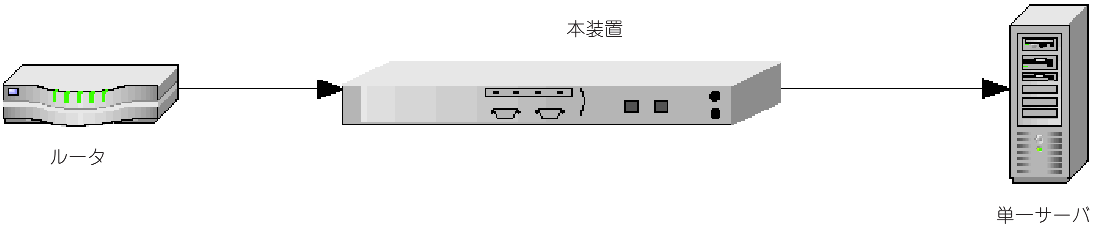


図3-1　単一サーバ構成

複数サーバ構成

本装置は、SSL処理を複数サーバ構成で行うときにも使用できます。複数サーバ構成では、本装置をルータとスイッチの間に接続します。サーバに向けて送信されたトラフィックを、本装置がいったん取り込み、処理を行います。その他のトラフィックはそのまま通過していきます。

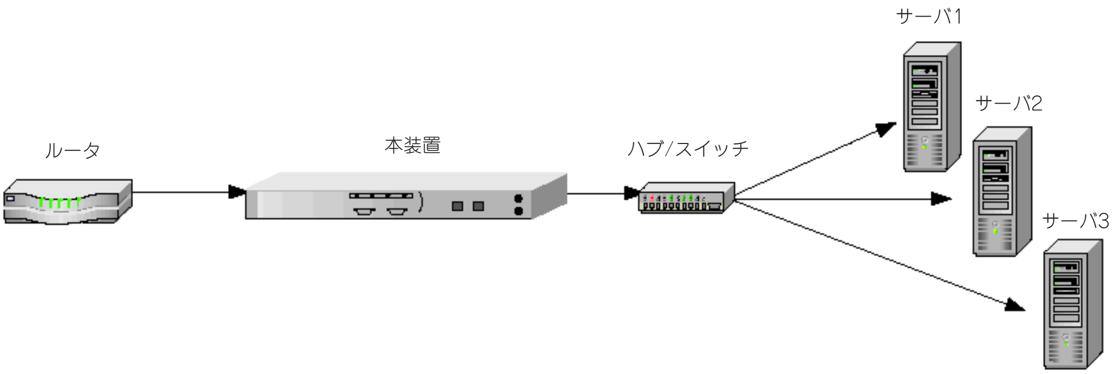


図3-2　複数サーバ構成

ITM(Internet Traffic Management)デバイスの操作

本装置には、ITM(Internet Traffic Management)デバイスとの互換性があります。ITMデバイスを使用する場合は、本装置をルータとITMデバイスの間に接続するか、ITMデバイスとサーバの間に接続します。ITMデバイスは、通信負荷を複数のサーバに分散させ、コンテンツごとにトラフィックを分類して分散させます。

ITMデバイス - クライアント・ネットワーク間への配置

ITMデバイスがレイヤ7のトラフィック管理をサポートしている場合は、トラフィック上のURLが読み取り可能(暗号化されていない)であることが必要です。このような環境では、本装置をITMデバイスとクライアント・ネットワークの間に配置することを推奨します。

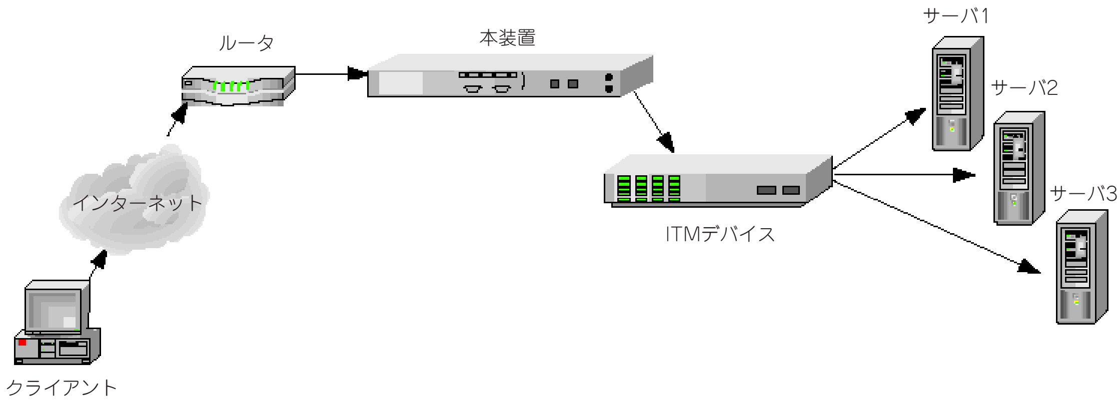


図3-3　ルータ - ITMデバイス間への配置

ITMデバイス - サーバ間への配置

セキュリティ要件で、暗号化されていないデータによる通信を制限している場合は、本装置をITMデバイスとサーバの間に配置する必要があります。

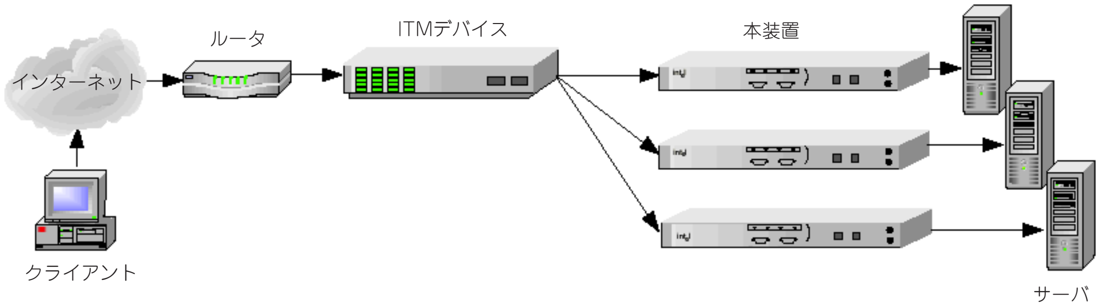


図3-4　ITMデバイス - サーバ間への配置

チェック

図3-4のこの構成を採用する場合は、レイヤ7のロードバランシングを行うことができません。この構成では、ITMデバイスを通過するセキュアトラフィックは暗号化されているからです。

複数の本装置をカスケード接続する場合

スケーラビリティとカスケード接続

複数の本装置をカスケード接続することにより、本装置の性能を拡張できます。カスケード接続では、前段の本装置のServer側ポートと後段のNetwork側ポートをケーブルで接続して、最後段に接続した本装置のServer側ポートをスイッチやサーバまたはITMデバイスに接続します。

Spill機能

本装置の「spill」(spillは「あふれ」と言う意味)オプションが有効になっている場合は、本装置がある特定の時間内でリクエストを処理しきれなかった場合、そのリクエストは処理されずそのまま暗号化された状態で次段のインライン状態の本装置に渡されます。また、最後段の本装置でも「spill」が有効になっていれば、同様に、そこで処理できなかったリクエストはそのままサーバに渡されることとなります。この「spill」機能は接続ごとに動的に動作し、つまり各装置ごと単独で、他の装置と連携せずに動作状態が決定されます(spillコマンドについては第5章「コマンド・リファレンス」を参照してください)。spill機能が無効になっている場合は、本装置「スロットル」状態になります。この場合、本装置は、過負荷状態が解消されるまで、着信した要求を受け入れません。

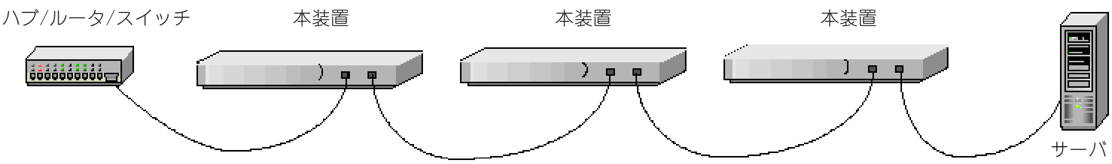


図3-5　カスケード接続

可用性(Availability)

フェイルスルー・モードが有効になっているとき、本装置に障害が発生するか、またはBypassモードに設定すると、本装置は、その機能がなんらかの原因によって停止した場合に、その2つのRJ-45コネクタを内部で直接接続し、停止状態が解除されるまで、トラフィックを何の処理もせずに通過させます。この機能により、単一の装置の故障がネットワーク全体に影響を与えるのを防止し、高いレベルの可用性を提供することが可能になります。また、前述したように、複数の本装置を用いる場合は、後段にカスケードされるユニットによって暗号化/復号化処理能力を追加することができます。また、単一の装置を用いる場合でも、サーバに処理の一部を任せることができます。詳細については、付録B 「障害/バイパス・モード」を参照してください。

鍵と電子証明書

本装置を使用するには、鍵と電子証明書が必要です。鍵は、データの暗号化/復号化に使用される一連の数値です。また、電子証明書は、サーバやユーザを特定化する「書類」です。電子証明書には、ユーザーの会社に関する情報のほか、ユーザーの身元を証明する第三者の情報も含まれています。
鍵と電子証明書は、次の3とおりの方法で取得できます。

- VeriSign社をはじめとする認証局から電子証明書を取得
- 既存の鍵/電子証明書を使用
- 新しい鍵/電子証明書を本装置で作成

重要 **本装置ではテスト用に電子証明書を作成することができますが、実際に使用する電子証明書は、認知されている認証局から取得する必要があります。**

ハイパーターミナルでのカット&ペースト

次のいくつかの手順では、カット&ペースト機能を使用します。ここでは、ハイパーターミナルを使用するものとしてカット&ペーストの方法を説明します。これ以外のターミナル・プログラムを使用する場合は、その製品のマニュアルに記載されている正しい手順を参照してください。
ハイパーターミナルからアイテム(鍵データ、証明書署名要求、証明書等)をコピーするには、次のようにします。

1. ハイパーターミナルウィンドウを開きます。
2. アイテムを選択して、クリック、ドラッグします。
3. アイテムを選択したら編集メニューを開き、コピーをクリックします(Ctrl - C)。
4. データの貼り付け先のウィンドウを開き、適切な位置にカーソルを置きます。
5. 編集メニューの貼り付けをクリックします(Ctrl - V)。

以上の操作は最初の1回のみ行います。
ハイパーターミナルにコピーしたアイテム(鍵データ、証明書署名要求、証明書等)を貼り付ける(ペーストする)には、次のようにします。

1. 適切なアプリケーション・ウィンドウ内のアイテムを表示し、クリックとドラッグによってそのアイテムを選択します。
2. アイテムを選択して編集メニューをクリックし、コピーを選択します。(Ctrl - C)
3. ハイパーターミナルウィンドウに移動し、適切な位置にカーソルを置きます。
4. 編集メニューのホスト側に貼り付けを選択します(Ctrl - V)。

VeriSign社をはじめとする認証局からの電子証明書の取得

create keyコマンドを使って鍵を作成します。create signコマンドを使って、署名要求(CSR)を作成します。作成した署名要求は、認証を受け署名をしてもらうために認証局(VeriSign社など)に送ります。すると、1〜5日間程度で署名済みの電子証明書が返送されてきます。この電子証明書を本装置にインポートするには、import certコマンドを使用します。

署名要求を作成するとき、各フィールドに入力した情報のことを総称的に「DN(Distinguished Name/識別名)」と呼びます。追加のセキュリティ機能を実現するために、DNが一意な値になるように、フィールドに入力した値の一部に変更が必要となる場合があります。

重要

鍵を作成した場合は、必ず設定を保存してください。設定の保存には、config saveコマンドを使用します。またexport keyコマンドでバックアップを作ることを推奨します。鍵が保存されていないと、取得した電子証明書が使えません。

鍵を作成するには、次のようにします。

1. プロンプトにcreate keyコマンドを入力します。

```
Intel 7110> create key
Key strength (512/1024) [512]:
New keyID [001]: 002
Keypair was created for keyID: 002
```

2. 電子証明書署名要求を作成します。

```
Intel 7110> create sign 002
You are about to be asked to enter information that will be incorporated
into your certificate request. The "common name" must be unique. For
other fields, you could use default values.
```

以下の説明に従い要求される項目に入力していきます。
各認証局が持つ固有のガイドラインに従って本装置からの問い合わせに回答することが必要です。こうしたガイドラインは認証局によって異なっているため、CSR(Certificate Signing Request/電子証明書署名要求)の送付先として選択した認証局のガイドラインを参照する必要があります。署名要求(CSR)に組み込む情報を入力するときは、次のことに注意してください。

- Country Code:　国名を表す2文字の略語。ISO形式(日本の場合はJP)となります。
- State or Province:　電子証明書を必要とする組織の本社がある州。州名を省略しないで入力してください(日本の場合は都道府県名)。
- Locality:　通常、組織の本社がある市
- Organization:　ドメイン名を所有している組織名(企業名、大学名、政府機関名など)です。行政区画(国、州、市など)レベルで登録されている正式な名前を使用してください。組織名の省略や、次の特殊文字の使用は不可です。 : < > ~ ! @ # $ % ^ * / ¥ ( ) ?
- Organization Unit:　通常、電子証明書を使用する部門またはグループの名前です。
- Common name:　サーバのDNSルックアップ処理で使用する「完全修飾ドメイン名(FQDN)」であり、URLとも呼ばれます(www.mysite.comなど)。ブラウザは、この情報を使ってWebサイトを確認します。ブラウザによっては、サーバ名と電子証明書に組み込まれているCommon nameが一致しないとき、安全なコネクションの確立を拒否するものもあります。Common nameには、プロトコル指定子「http://」やポート番号、パス名などを含めないでください。また、「*」、「?」などのワイルドカードやIPアドレスの使用は不可です。
- Email address:　電子証明書を管理する担当者の電子メールアドレス。

3. CSRをエクスポートします。

ここでは、コンソールポートに接続されているPCに、xmodemを使ってCSRを送る例を示します。

```
Intel 7110> export sign mywebserver
Export protocol: (xmodem, uuencode, ascii)
[ascii]:x <Enter>
Use Ctrl-x to kill transmission
Beginning export...
Export successful!
Intel 7110>
```

CSRを認証局に送る場合は、認証局が用意しているオンラインのフォームに、この結果表示される内容をコピーして貼り付けます。このときに、「----- BEGIN CERTIFICATE REQUEST -----」という行と「----- END CERTIFICATE REQUEST -----」という行も含めて貼り付けるようにしてください。

CSRの一般的な例は以下のようになります。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnDCCAQUACQAwXjELMAkGA1UEBhMCQ0ExEDOABgNVBAgTB
09udGFayW8xEDAOBgNVBAcTB01vbnRyYWwxDDAKBgNVBAoTA0
tGQzEdMBsGA1UEAxMUd3d3Lmlsb3ZlY2hpY2tlbi5jb20wgZ0
wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBALmJA2FLSGJ9iCF8
uwfPW2AKkyyKoe9aHnnwLLw8WWjhl[ww9pLietwX3bp6Do87m
wV3jrgQ1OIwarj9iKMLT6cSdeZ0OTNn7vvJaNv1iCBWGNypQv
3kVMMzzjEtOl2uGl8VOyeE7jImYj4HlMa+R168AmXT82ubDR2
ivqQwl7AgEDoAAwDQYJKoZIhvcNAQEEBQADgYEAn8BTcPg4Ow
ohGIMU2m39FVvh0M86ZBkANQCEHxMzzrnydXnvRMKPSE208x3
Bgh5cGBC47YghGZzdvxYJAT1vbkfCSBVR9GBxef6ytkuJ9YnK
84Q8x+pS2bEBDnw0D2MwdOSF1sBb1bcFfkmbpjN2N+hqrrvA0
mcNpAgk8nU=
-----END CERTIFICATE REQUEST-----
```

4. 認証局から返送されてきた署名済みの電子証明書を本装置にインポートします。import certコマンドにキーIDを指定して実行し、鍵のインポートに使用するプロトコルを選択します。ここでは、p(貼り付け)を選択します。最後にピリオドを3つ入力し、コマンドラインに戻ります。

```
Intel 7110> import cert mywebserver
keyid is mywebserver;
Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDELM
AkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQb3
dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
.
.
.
-----END CERTIFICATE----- <Enter>

... <Enter>
Import successful!
Intel 7110>
```

5. サーバ1のマッピングを作成します。create mapコマンドを使って、サーバのIPアドレス、ポート、鍵情報(キーID)を指定してください。

```
Intel 7110> create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: mywebserver
```

6. マッピングの作成後、設定を保存します。

```
Intel 7110> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

既存の鍵/電子証明書の使用

鍵/電子証明書をサーバからエクスポート

ここからは、既存の鍵と電子証明書を使用する方法について説明します。
鍵と電子証明書をエクスポートする方法の詳細については、サーバ・ソフトウェアのマニュアルを参照してください。エクスポートが完了したら、import keyコマンドとimport certコマンドを使って、鍵と電子証明書を本装置に貼り付けます。次に、Apache Web Server製品を使用する場合の一般的な処理方法を示します。
以下に示す手順は、システム構成の違いなどによって、異なる場合があります。特に環境変数($APACHROOT)が設定されていないことがあり、その際は各システムのApacheソフトウェアやSSLソフトウェアのインストール情報から同等の情報を判別する必要があります。

OpenSSLを用いたApache(mod_ssl)

鍵：

1. $APACHEROOT/conf/httpd.confファイルを参照して、*.keyファイル(鍵ファイル)の場所を調べます。
2. 鍵データをコピー&ペーストします。

電子証明書：

1. $APACHEROOT/conf/httpd.confファイルを参照して、*.crtファイル(電子証明書ファイル)の場所を調べます。
2. 電子証明書ファイルをコピー&ペーストします。

Apache SSL

鍵：

1. $APACHESSLROOT/conf/httpd.confファイルを参照して、*.keyファイル(鍵ファイル)の場所を調べます。
2. 鍵データをコピー&ペーストします。

電子証明書：

1. $APACHESSLROOT/conf/httpd.confファイルを参照して、*.certファイル(電子証明書ファイル)の場所を調べます。
2. 電子証明書ファイルをコピー&ペーストします。

stronghold

鍵：

1. $STRONGHOLDROOT/conf/httpd.confファイルを参照して、*.keyファイル(鍵ファイル)の場所を調べます。
2. 鍵データをコピー&ペーストします。

電子証明書：

1. $STRONGHOLDROOT/conf/httpd.confファイルを参照して、*.certファイル(電子証明書ファイル)の場所を調べます。
2. 電子証明書ファイルをコピー&ペーストします。

本装置へのインポート

1. import keyコマンドにキーIDを指定して実行し、インポートに使用するプロトコルを選択します。ここではデフォルトの「paste」を選択します。最後に改行マークの後にピリオドを3つ入力し、コマンドラインに戻ります。

```
Intel 7110> import key mywebserver
Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBALGOlBH14vIdtfuA+UnyRIoKya13ey8mj3GDQ
akdwoDJALu+jtcC
.
.
.
S9dPdwp6zctsZeztn/ewPeNamz3q8QoEhY8CawEA

-----END RSA PRIVATE KEY-----<Enter>

... <Enter>
Import successful!
Intel 7110>
```

2. import certコマンドにキーIDを指定して実行し、インポートに使用するプロトコルを選択します。ここでは、デフォルトの「paste」を選択します。最後に改行マークの後にピリオドを3つ入力し、コマンドラインに戻ります。

```
Intel 7110> import cert mywebserver
keyid is mywebserver;
Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDELM
AkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQb3
dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
.
.
.
-----END CERTIFICATE----- <Enter>

... <Enter>
Import successful!
Intel 7110>
```

3. サーバのマッピングを作成します。create mapコマンドを使って、サーバのIPアドレス、ポート、キーID(key ID)を指定してください。

```
Intel 7110> create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: mywebserver
```

4. マッピングの作成後、設定を保存します。

```
Intel 7110> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

新しい鍵/電子証明書の作成

create keyコマンドとcreate certコマンドを使って、本装置での処理に使用する新しい鍵と電子証明書を作成します。この方法は、サーバ上に鍵や電子証明書がない場合に選択できます。この方法には、鍵と電子証明書をすぐに取得できるという利点がありますが、認証局による署名はありません。

電子証明書を作成するとき、各フィールドに入力した情報のことを総称的に「DN(Distinguished Name/識別名)」と呼びます。追加のセキュリティ機能を実現するためには、DNが一意な値になるように、フィールドに入力した値の一部の変更が必要となる場合があります。

1. 次のようにして鍵を作成します。

```
Intel 7110> create key
Enter the key strength [512,1024]: 512
New keyID [001]: mywebserver
Keypair was created for keyID: mywebserver
```

2. create certコマンドにKeyIDを指定して実行します。

```
Intel 7110> create cert mywebserver
You are about to be asked to enter information?
```

電子証明書情報の入力を求めるプロンプトが表示されます。次の各情報を入力してください。

- Country Code (国コード)
- State or Province (都道府県名)
- Locality (市町村名)
- Organization (ドメイン名を所有している組織名)
- Organization Unit (部署名等)
- Common name (例：www.myserver.com)
- Email address (電子メールアドレス)

3. サーバのマッピングを作成します。create mapコマンドを使って、サーバのIPアドレス、ポート、キーID(KeyID)を指定してください。

```
Intel 7110> create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: mywebserver
```

4. マッピングの作成後、設定を保存します。

```
Intel 7110> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

グローバル・サイト電子証明書

概　要

ここでは、以下の4種類の電子証明書について説明します。

- ルートCA電子証明書。VeriSignなどの信頼できる認証局(CA)の電子証明書。
- サーバ電子証明書。サーバ上にロードされる、自己生成された電子証明書またはVeriSignなどの認証局から受け取った電子証明書。要求の発信元のブラウザが持つルートCA電子証明書との相互作用によって、暗号化通信のための認証が行われます。
- グローバル・サイト電子証明書。拡張されたサーバ電子証明書。米国国外への輸出向けに機能が制限されたブラウザでも128ビット暗号化を使用できるようにします。
- 中間認証局(中間CA)電子証明書。「他のCAによって署名されたCA」の電子証明書。VeriSignなどの公認の認証局によって認証され、グローバル・サイト電子証明書の有効性の確認に使用されます。以下の説明では、「中間CA電子証明書」と呼びます。

Internet ExplorerおよびNetscape Communicatorの米国国外向けの旧版は、40ビット暗号化を使用してSSLサーバにコネクションを張ります。SSLサーバは、クライアントからの要求を受信すると、電子証明書を返信します。この電子証明書が従来のサーバ電子証明書である(つまり、グローバル・サイト電子証明書ではない)場合は、ブラウザとサーバは、SSLハンドシェークを完了し、40ビット鍵を使用してアプリケーション・データを暗号化します。しかし、SSLサーバが要求の発信元のブラウザにグローバル・サイト電子証明書を返信した場合は、クライアントは、自動的に再度コネクションを張り、128ビット暗号化を使用します。

グローバル・サイト電子証明書は、それに対応する中間CA電子証明書とその中間CA電子証明書に署名をしたCAのルート電子証明書よって有効性が確認されます。(電子証明書の連鎖と呼びます。)中間CA電子証明書には、Microsoft SGC RootやVeriSign Class 3 CAなどがあります。ブラウザは、サーバに対して証明書を要求します。サーバは、その要求に対しグローバル・サイト電子証明書と対応する中間CA電子証明書を送ります。ブラウザは、受け取った中間CA電子証明書に署名しているルートCAの電子証明書をブラウザ内にあらかじめ登録されている電子証明書の中から探し有効性を確認します。この結果この中間CA証明書の有効性が確認され、そしてグローバル・サイト電子証明書の有効性が確認されます。有効性が確認されると128ビット暗号化通信が使用可能になります。

グローバル・サイト電子証明書の貼り付け手順

> ヒント
>
> 本装置は、1つのマッピングにつき1つのルートCA電子証明書と、1つのマッピングにつき複数の中間CA電子証明書をサポートします。

グローバル・サイト電子証明書を使用する場合は、グローバル・サイト電子証明書とそれに対応する中間CA電子証明書をインポートする必要があります。2つの電子証明書は、1つのファイルに結合されていなければなりません。

import certコマンドを使用して、単一の電子証明書や連鎖した複数の電子証明書をインポートできます。2つの連鎖した電子証明書を使用する場合は、最初にサーバのグローバル・サイト電子証明書を貼り付け、次に中間CAの電子証明書を貼り付けます。中間CAの電子証明書の後に改行してピリオドを3つ入力します。

ヒント

電子証明書の前後や2つの電子証明書の間にスペース文字があってはなりません。また、"Begin"ヘッダと"End..."トレーラは、すべてそのまま残しておかなければなりません。

例：

```
Intel 7110> import cert <keyID>
Import protocol: (paste, xmodem, uudecode)
[paste]:
Type or paste in data, end with ... alone on line
-----BEGIN CERTIFICATE-----
MIIFZTCCBM6gAwIBAgIQCTN2wvQH2CK+rgZKcTrNBzANBgkqh
kiG9w0BAQQFADCBujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1c3
QgTmV0d29yazEXMBUGA1UECxMOVmVyaVNpZ24sIEluYy4xMzA
xBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy
:
dmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlza
WduLmNvbS9DUFMg
SW5jb3JwLmJ5IFJlZi4gTElBQklMSVRZIExURC4oYyk5NyBWZ
XJpU2lnbjAeFw05
OTExMTEwMDAwMDBaFw0wMDExMTAyMzU5NTlaMIHHMQswCQYDV
QQGEwJVUzETMBEG
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIQI2yXHivGDQv5dGDe8QjDwzANBgkqh
kiG9w0BAQIFADBfMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVm
VyaVNpZ24sIEluYy4xNzA1BgNVBAsTLkNsYXNzIDMgUHVibGl
jIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcN
OTcwNDE3MDAwMDAwWhcN
:
OTk3IFZlcmlTaWduMA0GCSqGSIb3DQEBAgUAA4GBALiMmMMrS
PVyzWgNGrN0Y7uxWLaYRSLsEY3HTjOLYlohJGyawEK0Rak6+2
fwkb4YH9VIGZNrjcs3S4bmfZv9jHiZ/4PC/
NlVBp4xZkZ9G3hg9FXUbFXIaWJwfE22iQYFm8hDjswMKNXRjM
1GUOMxlmaSESQeSltLZl5lVR5fN5qu
-----END CERTIFICATE-----<Enter>
...<Enter>
Import successful!
Intel 7110>
```

リダイレクション：暗号方式をサポートしないクライアント

選択された暗号方式をサポートしないクライアントが本装置にコネクションを張ろうとした場合、デフォルトの動作では、そのコネクションが拒否されます。この場合、クライアント・システムは致命的エラーを報告します。しかし、本装置では、管理者が「リダイレクト・アドレス」を指定し、そのアドレスでクライアントに追加情報を提供することができます。set redirectコマンドを使用して、任意のマップIDに対してリダイレクトWebアドレスを指定できます。show redirectコマンドは、現在設定されているリダイレクト・アドレスをすべて表示します。

チェック　管理者は、リダイレクトURLを指定し、そのURLが使用可能であることを確認しなければなりません。また、リダイレクト・ページの内容を定義しておかなければなりません。

重要　**クライアントが、リダイレクトURLに従って、リダイレクションを発生させた本装置のマッピングと同じマッピングにアクセスした場合は、無限ループ状態が発生します。**

```
Intel 7110> list map

Map                Net  Ser  Cipher   Re-   Client
ID KeyID Server IP Port Port Suites   direct Auth

== ===== ========= ==== ==== ======   =====  ====

1  default Any     443  80   all(v2+v3) n   n
2  sample 10.1.2.5 443  80   med(v2+v3) n   n

Intel 7110> set redirect 2
Enter a redirect URL at following prompt
e.g. http://www.e-comm_site.com/weakbrowser.html

Enter redirect URL []:http://www.e-comm_site.com/
cipher_info.html

Intel 7110> list map

Map                Net  Ser  Cipher   Re-   Client
ID KeyID Server IP Port Port Suites   direct Auth

== ===== ========= ==== ==== ======   =====  ====

1  default Any     443  80   all(v2+v3) n    n
2  sample 10.1.2.5 443  80   med(v2+v3) y    n

Intel 7110> show redirect 2

Redirect URL for map 2 is set: http://www.e-
comm_site.com/cipher_info.html
```

特定のマッピングのリダイレクトURLを無効にするには、次のようなコマンドを使用します。

```
Intel 7110> set redirect 2 none
Intel 7110> show redirect 2
Redirect URL for map 2 is not set
```

クライアント認証

デフォルトでは、本装置はクライアントの認証をしません。ただし、クライアントを認証のためにクライアント電子証明書を要求するように、特定のマップIDを設定しておくことができます。この機能が有効になっている場合、本装置は、信頼しているCAがクライアント電子証明書に署名しているかどうかを確認します。この機能は、import client_caコマンドによって制御されます。

例：

最初に、list mapコマンドを使用して、現在のマップIDとそれらの設定を表示します。最後の項目は、クライアント認証機能が有効(y)になっているか無効(n)になっているのを示しています。

```
Intel 7110> list map

Map                Net  Ser  Cipher  Re-    Client

ID KeyID Server IP Port Port Suites  direct Auth

== ===== ========= ==== ==== ======  =====  ====

1 default Any       443  80  all(v2+v3) n      n

2 sample  10.1.2.57 443  80  med(v2+v3) n      n
```

次に、 マップID 2にクライアント用CA電子証明書をインポートします。

```
Intel 7110> import client_ca 2

Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>

Type or paste in data, end with ... alone on line

-----BEGIN CERTIFICATE-----

MIIDxzCCAzCgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBpDELM
AkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExEjAQBg
NVBAcTCVNhbiBEaWVnbzEUMBIGA1UE
.
.
.
XcCabZcfBRuYcZeUoNrGUl8tD80jp2YNG1vidgLEaD1YCli5I
9/mNrcB25mSfdAR

/08ROTMxm4VKOSA=

-----END CERTIFICATE-----<Enter>

...<Enter>
```

list mapコマンドをもう一度使用して、インポートの結果を確認します。Client Authの項目で、マップID 2のクライアント認証機能が有効になっていることに注意してください。

```
Intel 7110> list map

Map                   Net  Ser  Cipher   Re-    Client

ID KeyID Server IP Port Port Suites   direct Auth

== ===== ========= ==== ==== ======   =====   ====

1 default Any        443   80  all(v2+v3) n       n

2 sample  10.1.2.57 443   80  med(v2+v3) n       y
```

"map 2"にコネクションを張ろうとするクライアントは、上記の手順でインポートされた電子証明書が証明するCAが署名したクライアント電子証明書を提示するように要求されます。正しい署名を持つ電子証明書を提示しない場合は、コネクションは拒否されます。

操作の基本

OpenSSLを使用したクライアントCA電子証明書の作成

クライアント電子証明書を生成する際は、市販のソフトウェア・パッケージを使用できます。この作業は、手動で実行することもできます。以下の例は、OpenSSLを使用した手順を示しています。

ヒント

ユーザーの環境にOpenSSLのコピーを取得するには、OpenSSLのWebサイト(www.openssl.org)にアクセスします。

1. クライアントCA用の鍵のペアを生成します。

   ```
   openssl genrsa -out ca_key.pem 1024
   ```

2. クライアントCA電子証明書を生成します。

   ```
   openssl req -new -x509 -config intel.cnf -key ca_key.pem
   -days 365 -out ca_cert.pem
   ```

   ここではintel.cntはOpen SSL用のコンフィグレーション・ファイルです。作成方法についてはhttp://www.openssl.orgなどのサイトを参照してください。

3. import client_caコマンドを使用して、ca_cert.pemをインポートします。

各クライアントについて、以下の手順を実行します。

ヒント　この例では、ca_cert.pemは、信頼できるCAの署名済みの電子証明書です。

1. 鍵のペアを生成します。

   ```
   openssl genrsa -out key.pem 1024
   ```

2. 電子証明書署名要求を生成します。

   ```
   openssl req -new -config intel.cnf -days 365
   -key key.pem -out csr.pem
   ```

3. クライアントCA電子証明書を使用して、クライアント電子証明書署名要求に署名します。

   ```
   openssl x509 -req -CAcreateserial -CAkey ca_key.pem -CA ca_cert.pem -
   days 365 -in csr.pem -out cert.pem
   ```

4. 署名済みの電子証明書の形式をPEM形式からPKCS12形式に変換します。

   ```
   openssl pkcs12 -export -in cert.pem -inkey key.pem -name
   "<証明書識別名>" -out cert.p12
   ```

5. 手順4で得られた出力ファイル(署名済みの電子証明書cert.p12)を、クライアント・ブラウザにインポートします。

SSLの処理

本装置を使用することにより、複数のSSLプロトコルを処理できます。デフォルトのSSLプロトコルはHTTPSです。また、セキュリティ保護の目的で、特定のIPアドレスや特定のポートへのアクセスもブロックできます(「ブロック」を参照)。マッピングされないトラフィックやブロックされないトラフィックは透過的に受け渡されます(「障害発生時の処理-フェイルセーフとフェイルスルー」を参照)。
サポートされるプロトコルを以下に示します(任意の空きポートを使用できますが、ここでは一般的なポートの割り当てを示します)。

- HTTPS 443 (デフォルト)
- MAPS 993
- POP3S 995
- SMTPS 465
- NNTPS 563
- LDAPS 636

マッピング

鍵の組み合わせ(キーペア)と対応する電子証明書の識別にはキーID、サーバの識別にはサーバのIPアドレスとネットワークポート番号の組み合わせを使用します。マッピングとは、このキーIDとサーバ(サーバのIPアドレス、ネットワーク側ポート番号、サーバ側ポート番号を使用)を対応付ける処理のことです。本装置では、次の2種類のマッピングを行うことができます。

- 自動マッピング
- 手動マッピング

ヒント

最大100までのマッピングをサポートします。

自動マッピング

自動マッピングを行う場合は、サーバのIPアドレスとして0.0.0.0を指定します。このように指定すると、本装置はすべてのサーバに対する特定のポート番号(後述のデフォルト)へのパケットに割り込むようになります。マッピング・エントリを作成するときは、サーバのIPアドレスとネットワーク側ポート番号の組み合わせが他のエントリと重複しないように注意してください。

重要

マッピングを変更した場合は、必ず設定を保存してください。設定の保存には、config saveコマンドを使用します。

本装置の出荷時の設定では、ネットワーク側ポート443とサーバ側ポート80の自動マッピング・エントリが用意されています。この自動マッピングエントリは、内部で生成されたデフォルトのキーペアと電子証明書(キーIDは「default」)に対応しています。この設定では、トラフィックが本装置を介して送信されるとき、ネットワーク側ポート443のすべてのサーバで自動マッピングが行われます。

ユーザー指定の鍵と電子証明書を使った自動マッピング

自動マッピングに使用する鍵と電子証明書をユーザーが指定する場合は、create mapコマンドを使って、初期設定の自動マッピング・エントリを新しいエントリで置き換えます。初期設定の自動マッピング・エントリを新しいエントリで上書きするには、同じ一意の識別子(サーバのIPアドレス 0.0.0.0、ネットワーク側ポート443)とユーザーが作成したキーIDを指定します。使用する鍵と電子証明書の取得方法に特に制限はありません(この章で説明した取得方法のうちいずれかを使用)。

複数のポートを組み合わせた自動マッピング

ネットワーク側ポート番号が一意であれば、複数の自動マッピング・エントリを指定できます。たとえば、初期設定時のネットワーク側ポート(443)とサーバ側ポート(80)のほかに、ネットワーク側ポート(8010)とサーバ側ポート(80)の組み合わせを指定できます。

自動マッピング・エントリの削除

自動マッピング・エントリは自由に削除できます。ただし、他のマッピング・エントリを作成していない状態で初期設定時の自動マッピング・エントリを削除すると、自動マッピング・エントリが自動的に再生成されます。初期設定時の自動マッピング・エントリを削除するには、このエントリを新しいエントリで置き換えるか、別のマッピング(自動マッピング)エントリを作成してからdelete mapコマンドを実行します。

手動マッピング

create mapコマンドを使って、サーバごとに1つ以上のマッピング・エントリを手動でも作成できます。各サーバに一意のキーIDを指定するには、この方法を利用します。通常、手動マッピングを作成した場合は、デフォルトの自動マッピング・エントリを削除します。

自動マッピングと手動マッピングの組み合わせ

自動マッピングと手動マッピングで作成したエントリを組み合わせて、最大100のエントリまで使用できます。ただし、この場合は、サーバIPアドレス、ネットワーク側ポートの組み合わせが一意でなければなりません。実際のマッピング手順については、第4章「設定例」で詳しく説明します。

チェック　手動マッピングと自動マッピングの両方を使用できる場合は、本装置は常に手動マッピングを使用します。

ブロック

本装置では、セキュリティ保護の目的で、指定のIPアドレスの指定のポートに対するブロックを行うことができます。この処理は、次の情報に基づいて行われます。

- 指定のIPアドレスの指定のポート
- サブネットのIPアドレス、指定のポート
- すべてのIPアドレス、指定のポート

チェック　ブロックは、常にマッピングの前に実行されます。

指定のIPアドレスの指定のポートに対するブロック

特定のサーバのIPアドレスとポートの組み合わせをブロックするには、次のようにします。

1. create blockコマンドを入力します。
2. IPアドレスを入力します。
3. Enterキーを押し、デフォルトのIPワイルドカード・マスクを受け入れます。
4. 指定したいポート番号を入力します。
5. Enterキーを押し、デフォルトのポート・マスクを受け入れます。

例：

```
Intel 7110> create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.255.255
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [0.0.0.0]: 255.255.255.255
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

確認には、show blockコマンドを使用します。

```
Intel 7110> show block
(1) block 10.1.2.1 255.255.255.255 20.1.2.1
255.255.255.255 80 0xffff
```

指定のサブネットの指定のポートに対するブロック

サブネットのIPアドレス、特定のポートの組み合わせをブロックするには、次のようにします(この設定では、特定のサブネット上の全てのホストの特定のポートへのトラフィックをブロックします)。

1. サブネットIPアドレスを入力します。末尾の値は0にします(正確にはサブネットのサイズに合わせて、サブネットサイズ分の下位ビット値を0とした値を入力します)。この例では、ポート80の「10.1. x .x」〜「20.1. x .x」ではじまるIPアドレスがすべてブロックされます。
2. サブネットマスクを入力します。ビット値に変換した後に0となるビットのIPアドレス部分を無視することを示しています。
3. 特定のポートを入力します。
4. Enterキーを押し、デフォルトのポート・マスクを受け入れます。

例：

```
Intel 7110> create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.0.0
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [0.0.0.0]: 255.255.0.0
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

確認には、show blockコマンドを使用します。

```
Intel 7110> show block
-----------
blocks :
-----------
(1) block 10.1.2.1 255.255.0.0 20.1.2.1
255.255.0.0 80 0xffff
-----------
```

すべてのIPの指定のポートに対するブロック

すべてのIPアドレスの指定のポートに対してブロックするには、次のようにします。

1. ブロック対象のIPアドレスとして、0.0.0.0を入力します。
2. ブロック対象のIPワイルドカード・マスクとして、0.0.0.0を入力します。
3. 指定のポートを入力します。
4. Enterキーを押し、デフォルトのポート・マスクを受け入れます。

例：

```
Intel 7110> create block
Client IP to block [0.0.0.0]: <enter>
Client IP mask [0.0.0.0]: <enter>
Server IP to block [0.0.0.0]:<enter>
Server IP mask [0.0.0.0]:<Enter>
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

確認には、show blockコマンドを使用します。

```
Intel 7110> show block
-----------
blocks :
-----------
(1) block
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 80 0xffff
-----------
```

操作の基本

ブロックの削除

次の例では、ブロック定義を削除する方法を示します。ブロック定義を削除するには、delete blockコマンドにブロックIDを指定して実行します。この例の場合、ブロックIDは1です。

1. show blockコマンドを実行し、削除するブロックを特定します。

   ```
   Intel 7110> show block
   -----------
   blocks :
   -----------
   (1) block 10.1.2.1 255.255.255.255 20.1.2.1
   255.255.255.255 80 0xffff
   -----------
   ```

2. delete blockコマンドに、削除するブロックIDを指定して実行します。

   ```
   Intel 7110> delete block 1
   ```

マスク値の意味

ブロックコマンドによるIP maskやPort maskは設定IP値やport値が<value>であり、通過しようとするトラフィックのIP値やport値が<passing-value>の/でマスク値が<mask>の場合、<passing-value>AND<msak>=<value>AND<mask>が成立する場合に条件が有効になります。

障害発生時の処理 - フェイルセーフとフェイルスルー

本装置で障害が発生した場合に未処理のデータパケットを通過させるかどうかは、フェイルセーフ・モードとフェイルスルー・モードのどちらを使用しているかによって決定します。フェイルスルー・スイッチは、デフォルトではフェイルセーフ・モードに設定されています。このモードでは、障害が発生している間、データ・パケットは本装置を通過しません。詳細については、付録Bの「障害/バイパス・モード」を参照してください。